

2121
#2
KWS
7-23-01

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Virgil D. Gligor et al.



BLOCK ENCRYPTION METHOD
AND SCHEMES FOR DATA
CONFIDENTIALITY AND
INTEGRITY PROTECTION

No.: 09/761,771

Filing Date: 01/18/2001

Examiner: Unassigned

Art Unit: Unassigned

RECEIVED
JUL 19 2001
Technology Center 2100

INFORMATION DISCLOSURE STATEMENT
UNDER 37 CFR §1.56

Commissioner for Patents
Washington, D.C. 20231

Sir:

Submitted herewith on Form PTO-1449 is a listing of documents known to Applicants in order to comply with Applicants' duty of disclosure pursuant to 37 CFR §1.56. A copy of each listed document is being submitted to comply with the provisions of 37 CFR §1.97 and §1.98.

The submission of any document herewith, which is not a statutory bar, is not intended as an admission that such document constitutes prior art against the claims of the present application or that such document is considered material to patentability as defined in 37 CFR §1.56(b). Applicants do not waive any rights to take any action which would be appropriate to antedate or otherwise remove as a competent reference any document which is determined to be a *prima facie* art reference against the claims of the present application.

TIMING OF THE DISCLOSURE

The listed documents are being submitted in compliance with 37 CFR §1.97(b), before the mailing date of the first Office Action on the merits.

RELEVANCE OF EACH DOCUMENT

The relevance of Documents A1 – A15 is described in the present specification.

Applicants respectfully request that any listed document be considered by the Examiner and be made of record in the present application and that an initialed copy of Form PTO-1449 be returned in accordance with MPEP §609.


The Commissioner is hereby authorized to charge any additional fees which may be required regarding this application under 37 C.F.R. §§ 1.16-1.17, or credit any overpayment, to Deposit Account No. 19-0741. Should no proper payment be enclosed herewith, as by a check being in the wrong amount, unsigned, post-dated, otherwise improper or informal or even entirely missing, the Commissioner is authorized to charge the unpaid amount to Deposit Account No. 19-0741.

Respectfully submitted,

Date July 17, 2001

FOLEY & LARDNER
Washington Harbour
3000 K Street, N.W., Suite 500
Washington, D.C. 20007-5109
Telephone: (202) 672-5485
Facsimile: (202) 672-5399

By



William T. Ellis
Attorney for Applicant
Registration No. 26,874

Form PTO-1449 (MODIFIED)		U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE		ATTY. DOCKET NO. 068398-0102		SERIAL NO. 09/761,771	
INFORMATION DISCLOSURE CITATION (Use several sheets if necessary)				APPLICANT Virgil D. Gligor et al.			
				FILING DATE 01/18/2001		GROUP ART UNIT Unassigned	
U.S. PATENT DOCUMENTS							
EXAMINER INITIAL	REF	DOCUMENT NUMBER	DATE	NAME	CLASS	SUB- CLASS	FILING DATE IF APPROPRIATE
FOREIGN PATENT DOCUMENTS							
		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUB- CLASS	TRANSLATION YES NO
OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)							
	A1 /	A.J. Menezes et al, "Hash Functions and Data Integrity", Handbook of Applied Cryptography, Chp 7, pp 223-282; Chp 9, pp 321-383, 1997; CRC Press, Boca Raton					
	A2	Gligor et al, "Object Migration and Authentication", IEEE Transactions on Software Engineering SE-5, vol. 5, pp. 607-611, 1979, IEEE					
	A3	NBS FIPS Pub 46, titled "Data Encryption Standard", National Bureau of Standards, U.S. Dept of Commerce January 1977, pp. 1-18					
	A4	NBS FIPS Pub 81, Titled "DES Modes of Operation", National Bureau of Standards, U.S. Dept of Commerce pp. 1-17, December 1980					
	A5	Meyer et al, Cryptography; A New Dimension in Computer Data Security", A Guide For The Design and Implementation of Secure Systems, pp. 69-71, 1982, John Wiley & Sons, 2 nd printing					
	A6	Bellare et al, "A Concrete Security Treatment of Symmetric Encryption", Proceedings of the 38 th Symposium on Foundations of Computer Science, IEEE, 1997, pp. 394-403					
	A7	C.M. Campbell, "Design and Specification of Cryptographic Capabilities", in Computer Science And The Data Encryption Standard, (D.K. Brandstad (ed.) National Bureau of Standards Special Publications 500-527 U. S. Dept of Commerce, February 1978, pp. 54-66					
	A8	Naor et al, "From Unpredictability to Indistinguishability: A Simple Construction of Pseudo-Random Functions From MACs", in Advances in Cryptolog - CRYPTO '98 (LNCS 1462), pp. 267-282, 1998, Springer-Verlag					
	A9	Goldwasser et al, "Lecture Notes on Cryptography", 1999, Available at http://www.cse.ucsd.edu/users/mihir/papers/gb.pdf					
	A10	Kohl et al, RFC 1510, The Kerberos Network Authentication Service (V5)", Internet Request For Comments 1510					
EXAMINER				DATE CONSIDERED			
* EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include any copy of this form with next communication to applicant.							

July 17, 2001

Form PTO-1449 (MODIFIED)		U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE		ATTY. DOCKET NO. 068398-0102		SERIAL NO. 09/761,771	
INFORMATION DISCLOSURE CITATION <i>(Use several sheets if necessary)</i>				APPLICANT Virgil D. Gligor et al.			
				FILING DATE 01/18/2001		GROUP ART UNIT Unassigned	
U.S. PATENT DOCUMENTS							
EXAMINER INITIAL	REF	DOCUMENT NUMBER	DATE	NAME	CLASS	SUB- CLASS	FILING DATE IF APPROPRIATE
FOREIGN PATENT DOCUMENTS							
	REF	DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUB- CLASS	TRANSLATION YES NO
OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)							
	A11	Petrack et al, "CBC MAC for Real-Time Data Sources:, Manuscript Available at http://www.cs.technion.ac.il/~erez/publications.html , 1999					
	A12	Jueneman et al, "Message Authentication with Manipulation Detection Codes", Proc. Of the IEEE Symp. on Security and Privacy, Oakland, CA, pp. 33-54, 1983, IEEE Computer Society					
	A13	Stubblebine et al, "On Message Integrity in Cryptographic Protocols", Proceedings of the 1992 IEEE Computer Society Symposium on Research in Security and Privacy, pp. 85-104, 1992, IEEE Computer Society Press					
	A14	Kohl et al, "The use of Encryption in Kerberos for Network Authentication", Advances in Cryptology-CRYPTO 1989, (LNCS 435), pp. 35-43, 1990, Digital Equip. Corp.					
	A15	D. E. Knuth, "The Art of Computer Programming – Volume 2: Seminumerical Algorithms", 1981, (2 nd ed.) Chapter 3, pp. 1-110, Addison-Wesley					
EXAMINER				DATE CONSIDERED			
* EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include any copy of this form with next communication to applicant.							

July 17, 2001